C. REMARKS

Status of the Claims

Claims 1-20 are pending in the present application. Claims 1, 8, 14, and 19 were amended. No claims have been cancelled or added in this Response. Reconsideration of the claims is respectfully requested.

Examiner Interview

Applicants would like to thank Examiner Baum for his courtesy in holding the telephone interview of October 6, 2004 between the Examiner and the Applicants' Representative Attorney.

Drawings

Applicants note that the Examiner did not indicate whether Applicants' formal drawings, filed with the Application, are acceptable. Applicants respectfully request that the Examiner indicate whether the drawings are acceptable in the next Office Communication.

35 U.S.C. § 112, Second Paragraph

The Examiner has rejected claim 19 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that Applicants regard as the invention. This rejection is respectfully traversed.

Specifically, the Examiner stated:

> Claim 19 recites the limitation "A computer program product ... claim 5". There is insufficient antecedent basis for this limitation in the claim. The examiner assumes for the sake of applying art that the "claim 5" phrase should be "claim 18".

Applicants concur with the Examiner's observation that claim 19 is properly dependent upon claim 18. Accordingly, Applicants have amended claim 19 to recite a dependency on claim 18, thus obviating the Examiner's rejection.

Therefore, Applicants respectfully request that the rejection of claim 19 under 35 U.S.C. § 112, first paragraph be withdrawn.

35 U.S.C. § 102, Alleged Anticipation

The Examiner has rejected claims 1-20 under 35 U.S.C. § 102 as being anticipated by U.S. 5,983,350 to Minnear et al. This rejection is respectfully traversed.

With respect to claim 1, which is representative of the other rejected claims, the Examiner stated:

> As per claim 1: "A method of establishing a secure communication path between a computer system and a remote computer system comprising: exchanging identification data with the remote computer system using a communication path [col. 3, lines 35-col. 18, line 48]:
> determining, based on the identification data. whether a predefined security policy exists corresponding to the remote computer system [col. 3, lines 35-col. 18, line 48, whereas the SA aspects of IPSEC parameters clearly associate remote host identification data to communications security policy.]; and establishing a secure communication path using

> a default security policy in response to determining that the predefined security policy does not exist [col. 3,lines 35-col. 18,line 48, whereas the different levels of security, insofar as the setup of boot default values, constitutes a default protection level for establishing secure communication.].";

During the October 6, 2004 interview, the Examiner and Applicants' Representative discussed the above rejection under Section 102. As discussed in the interview, the Examiner interprets the term "security policy" as encompassing a security association (SA) under the IPSec (IP Security Protocol) standard, at least for purposes of examination (under the "broadest reasonable interpretation" standard). Applicants respectfully submit, however, that the present application refers to both SAs and "security policies" and recognizes a distinction between the two terms.

Specifically, the security policies described in the present application's specification actually impose constraints upon SAs that are created in accordance with a particular security policy. For example, consider the following excerpt from the specification, in which a "Phase 1 Security Policy" defines minimum and maximum lifetimes and lifesizes for SAs:

> The Phase 1 Security Policy information includes the following:
>
> - Phase 1 Security Policy Name, used as a database search key.
> - Initiator Proposal List Index - an index to a initiator proposal list record (see Proposal List **725**, below). If the Initiator Proposal List Index is null then initiation with the remote ID is not

allowed (i.e., the system only acts as a responder to the remote ID).

- Responder Proposal List Index - an index to a responder proposal list record (see Proposal List **725**, below). If this value is null, then response is not allowed (i.e., system only acts as an initiator when dealing with the remote ID). If both the Initiator Proposal List Index and the Responder Proposal List Index values are null, then no negotiation is allowed between the systems.
- Negotiation Mode - ISAKMP Main (normal negotiation) or Aggressive (faster negotiation).
- Minimum SA Lifesize - the security association lifesize in Kbytes, the lowest value is accepted as a responder.
- Minimum SA Lifetime - the security association lifetime in seconds, the lowest value is accepted as a responder.
- Default SA Lifesize - the security association lifesize in Kbytes used as a default if all associated transforms have 0 SA lifesize.
- Default SA Lifetime - the security association lifetime in seconds used as a default if all associated transforms have 0 SA lifetime.
- SA Refresh Threshold - an integer representing the percentage of SA life left at which a refresh is requested.
- Phase 1 Tunnel Time-of-Day - a string containing a start and stop time using a 24 hour clock. For example, "0800-1730" would allow the tunnel to exist from 8:00AM to 5:30PM. This parameter is used to determine the times during which the tunnel is allowed to exist.

- Phase 1 Tunnel Day(s) of week - a string containing a number representing the days of the week that the tunnel can be active. For example, "0,1,3" would allow the tunnel to be active on Sunday, Monday, and Wednesday. This parameter determines which days a tunnel is allowed to exist.

[Applicants' specification, p. 21, line 24 - p. 23, line 16].

Accordingly, Applicants have amended independent claims 1, 8, and 14 to recite limitations "wherein the predefined security policy defines at least one constraint on security associations (SAs) created in accordance with the predefined security policy" and "wherein the default security policy defines at least one constraint on security associations (SAs) created in accordance with the default security policy." These amendments clearly distinguish the term "security policy" from the term "security association," since the amendments now explicitly recite a distinguishing relationship between the two features. Thus, the rejection of independent claims 1, 8, and 14, which depended upon the term "security policy" encompassing a security association, has been obviated.

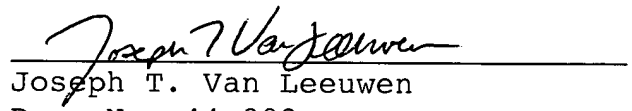
Claims 2-7, 9-13, and 15-20 are dependent claims that depend from independent claims 1 8, and 14. Applicants have already demonstrated claims 1 8, and 14 to be in condition for allowance. Applicants respectfully submit that claims 2-7, 9-13, and 15-20 are also allowable, at least by virtue of their dependency on allowable claims. Thus, Applicants respectfully request that the rejection of claim 1-20 under 35 U.S.C. § 102 be withdrawn.

Conclusion

As a result of the foregoing, it is asserted by Applicants that the remaining claims in the Application are in condition for allowance, and Applicants respectfully request allowance of such claims.

Applicants respectfully request that the Examiner contact the Applicants' attorney listed below if the Examiner believes that such a discussion would be helpful in resolving any remaining questions or issues related to this Application.

Respectfully submitted,

By 

Joseph T. Van Leeuwen
Reg. No. 44,383
Van Leeuwen & Van Leeuwen
Attorneys for Applicant
Telephone: (512) 301-6738
Facsimile: (512) 301-6742